EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	717	(713/171).CCLS.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/04/13 19:18
L2	96	spelman.IN.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/04/13 19:23
L3	2	("5638445").PN.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/04/13 20:23
L4	2	("4759063").PN.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/04/13 20:23

PORTAL
USPTO

Subscribe (Full Service) Register (Limited Service, Free) Login

Search: ● The ACM Digital Library ○ The Guide

blind encryption SEARCH

THE ACM DIGITAL LIBRARY

Feedback Report a problem Satisfaction survey

Terms used **blind encryption**

Found **5,024** of **199,915**

Sort results by: relevance

Display results: expanded form

Save results to a Binder

Search Tips

□ Open results in a new window

Try an Advanced Search
Try this search in The ACM Guide

Results 1 - 20 of 200

Result page: **1** 2 3 4 5 6 7 8 9 10 next

Best 200 shown

Relevance scale □▭▬■■

1 A resolution strategy for verifying cryptographic protocols with CBC encryption and blind signatures
Véronique Cortier, Michael Rusinowitch, Eugen Z□linescu
July 2005 **Proceedings of the 7th ACM SIGPLAN international conference on Principles and practice of declarative programming PPDP '05**
Publisher: ACM Press
Full text available: pdf(214.71 KB) Additional Information: full citation, abstract, references, index terms, review

Formal methods have proved to be very useful for analyzing cryptographic protocols. However, most existing techniques apply to the case of abstract encryption schemes and pairing. In this paper, we consider more complex, less studied cryptographic primitives like CBC encryption and blind signatures. This leads us to introduce a new fragment of Horn clauses. We show decidability of this fragment using a combination of several resolution strategies.As a consequence, we obtain a new decidability re ...

Keywords: cryptographic protocols, horn clauses, resolution strategies, verification

2 Strength of two data encryption standard implementations under timing attacks
Alejandro Hevia, Marcos Kiwi
November 1999 **ACM Transactions on Information and System Security (TISSEC)**, Volume 2 Issue 4
Publisher: ACM Press
Full text available: pdf(183.73 KB) Additional Information: full citation, abstract, references, citings, index terms, review

We study the vulnerability of two implementations of the Data Encryption Standard (DES) cryptosystem under a timing attack. A timing attack is a method, recently proposed by Paul Kocher, that is designed to break cryptographic systems. It exploits the engineering aspects involved in the implementation of cryptosystems and might succeed even against cryptosys-tems that remain impervious to sophisticated cryptanalytic techniques. A timing attack is, essentially, a way of obtaining some users ...

Keywords: cryptanalysis, cryptography, data encryption standard, timing attack

3 Multi-agent systems and social behavior: Blind sales in electronic commerce
E. Aïmeur, G. Brassard, F. S. Mani Onana

March 2004 **Proceedings of the 6th international conference on Electronic commerce ICEC '04**
Publisher: ACM Press
Full text available: pdf(330.05 KB) Additional Information: full citation, abstract, references, citings

We start with the usual paradigm in electronic commerce: a consumer who wants to buy from a merchant. However, both parties wish to enjoy maximal privacy. In addition to remaining anonymous, the consumer wants to hide her browsing pattern and even the identification of the product she may decide to buy. Nevertheless, she wants to be able to negotiate the price, pay, receive the product and even enjoy maintenance on it. On the other hand, the merchant wants to leak as little information as possib ...

Keywords: CAPTCHA, anonymous surfing, cryptography, customer buying behaviour, electronic commerce, oblivious transfer, private information retrieval

4 Data privacy and security: Simultaneous scalability and security for data-intensive web applications
Amit Manjhi, Anastassia Ailamaki, Bruce M. Maggs, Todd C. Mowry, Christopher Olston, Anthony Tomasic
June 2006 **Proceedings of the 2006 ACM SIGMOD international conference on Management of data SIGMOD '06**
Publisher: ACM Press
Full text available: pdf(275.45 KB) Additional Information: full citation, abstract, index terms

For Web applications in which the database component is the bottleneck, scalability can be provided by a third-party Database Scalability Service Provider (DSSP) that caches application data and supplies query answers on behalf of the application. Cost-effective DSSPs will need to cache data from many applications, inevitably raising concerns about security. However, if all data passing through a DSSP is encrypted to enhance security, then data updates trigger invalidation of large regions of ca ...

5 Distributed collaborative key agreement and authentication protocols for dynamic peer groups
Patrick P. C. Lee, John C. S. Lui, David K. Y. Yau
April 2006 **IEEE/ACM Transactions on Networking (TON)**, Volume 14 Issue 2
Publisher: IEEE Press
Full text available: pdf(837.49 KB) Additional Information: full citation, abstract, references, index terms

We consider several distributed collaborative key agreement and authentication protocols for dynamic peer groups. There are several important characteristics which make this problem different from traditional secure group communication. They are: 1) distributed nature in which there is no centralized key server; 2) collaborative nature in which the group key is contributory (i.e., each group member will collaboratively contribute its part to the global group key); and 3) dynamic nature in which ...

Keywords: authentication, dynamic peer groups, group key agreement, rekeying, secure group communication, security

6 Short papers: Specifying electronic voting protocols in typed MSR
Theodoros Balopoulos, Stefanos Gritzalis, Sokratis K. Katsikas
November 2005 **Proceedings of the 2005 ACM workshop on Privacy in the electronic society WPES '05**
Publisher: ACM Press
Full text available: pdf(141.00 KB) Additional Information: full citation, abstract, references, index terms

Electronic voting, as well as other privacy-preserving protocols, use special cryptographic primitives and techniques that are not widely used in other types of protocols, e.g. in authentication protocols. These include blind signatures, commitments, zero-knowledge proofs, mixes and homomorphic encryption. Furthermore, typical formalizations of the Dolev-Yao intruder's capabilities do not take into account these primitives and techniques, nor do they consider some types of attacks that e-voting ...

Keywords: Dolev-Yao intruder, electronic voting, privacy, security protocols, specification, typed MSR

7 Physical privacy: Privacy management for portable recording devices

J. Alex Halderman, Brent Waters, Edward W. Felten

October 2004 **Proceedings of the 2004 ACM workshop on Privacy in the electronic society WPES '04**

Publisher: ACM Press

Full text available: pdf(321.69 KB) Additional Information: full citation, abstract, references, index terms

The growing popularity of inexpensive, portable recording devices, such as cellular phone cameras and compact digital audio recorders, presents a significant new threat to privacy. We propose a set of technologies that can be integrated into recording devices to provide stronger, more accurately targeted privacy protections than other legal and technical measures now under consideration. Our design is based on an informed consent principle, which it supports by the use of novel devices and pr ...

Keywords: camera phones, privacy, recording devices

8 Unlinkable serial transactions: protocols and applications

Stuart G. Stubblebine, Paul F. Syverson, David M. Goldschlag

November 1999 **ACM Transactions on Information and System Security (TISSEC)**, Volume 2 Issue 4

Publisher: ACM Press

Full text available: pdf(184.87 KB) Additional Information: full citation, abstract, references, citings, index terms, review

We present a protocol for unlinkable serial transactions suitable for a variety of network-based subscription services. It is the first protocol to use cryptographic blinding to enable subscription services. The protocol prevents the service from tracking the behavior of its customers, while protecting the service vendor from abuse due to simultaneous or cloned use by a single subscriber. Our basic protocol structure and recovery protocol are robust against failure in protocol termination. ...

Keywords: anoymity, blinding, cryptographic protocols, unlinkable serial transactions

9 Improved proxy re-encryption schemes with applications to secure distributed storage

Giuseppe Ateniese, Kevin Fu, Matthew Green, Susan Hohenberger

February 2006 **ACM Transactions on Information and System Security (TISSEC)**, Volume 9 Issue 1

Publisher: ACM Press

Full text available: pdf(331.59 KB) Additional Information: full citation, abstract, references, index terms

In 1998, Blaze, Bleumer, and Strauss (BBS) proposed an application called *atomic proxy re-encryption*, in which a semitrusted proxy converts a ciphertext for Alice into a ciphertext for Bob *without* seeing the underlying plaintext. We predict that fast and secure re-encryption will become increasingly popular as a method for managing encrypted file systems. Although efficiently computable, the wide-spread adoption of BBS re-encryption has been hindered by considerable security risks. ...

Keywords: Proxy re-encryption, bilinear maps, double decryption, key translation

10 Teaching secure communication protocols using a game representation
Leonard G. C. Hamey
January 2003 **Proceedings of the fifth Australasian conference on Computing education - Volume 20 ACE '03**
Publisher: Australian Computer Society, Inc.
Full text available: pdf(252.19 KB) Additional Information: full citation, abstract, references, index terms

The Security Protocol Game is a highly visual and interactive game for teaching secure data communication protocols. Students use the game to simulate protocols and explore possible attacks against them. The power of the game lies in the representation of secret and public key cryptography. Specifically, the game provides representations for plain text and encrypted messages, message digests, digital signatures and cryptographic keys. Using these representations, students can construct public ke ...

Keywords: PGP, blind signature, computer network, cryptography, digital signature, key exchange, man-in-the-middle attack, protocols, replay attack, secure communication

11 A survey of key management for secure group communication
Sandro Rafaeli, David Hutchison
September 2003 **ACM Computing Surveys (CSUR)**, Volume 35 Issue 3
Publisher: ACM Press
Full text available: pdf(346.27 KB) Additional Information: full citation, abstract, references, citings, index terms

Group communication can benefit from IP multicast to achieve scalable exchange of messages. However, there is a challenge of effectively controlling access to the transmitted data. IP multicast by itself does not provide any mechanisms for preventing nongroup members to have access to the group communication. Although encryption can be used to protect messages exchanged among group members, distributing the cryptographic keys becomes an issue. Researchers have proposed several different approach ...

Keywords: Group Key Distribution, Multicast Security

12 Receipt-free secret-ballot elections (extended abstract)
Josh Benaloh, Dwight Tuinstra
May 1994 **Proceedings of the twenty-sixth annual ACM symposium on Theory of computing STOC '94**
Publisher: ACM Press
Full text available: pdf(1.09 MB) Additional Information: full citation, references, citings, index terms

13 Technical opinion: The viability of supporting anonymous employees
John Gerdes
April 2004 **Communications of the ACM**, Volume 47 Issue 4
Publisher: ACM Press
Full text available: pdf(62.86 KB) html(14.64 KB) Additional Information: full citation, abstract, index terms

Identifying contractual mechanisms to support anonymity in the employment environment.

14 Revokable and versatile electronic money (extended abstract)
Markus Jakobsson, Moti Yung
January 1996 **Proceedings of the 3rd ACM conference on Computer and communications security CCS '96**
Publisher: ACM Press
Full text available: pdf(1.53 MB) Additional Information: full citation, references, citings, index terms

15 Verifiable encryption of digital signatures and applications
Giuseppe Ateniese
February 2004 **ACM Transactions on Information and System Security (TISSEC)**, Volume 7 Issue 1
Publisher: ACM Press
Full text available: pdf(258.12 KB) Additional Information: full citation, abstract, references, index terms

This paper presents a new simple schemes for verifiable encryption of digital signatures. We make use of a trusted third party (TTP) but in an *optimistic* sense, that is, the TTP takes part in the protocol only if one user cheats or simply crashes. Our schemes can be used as primitives to build efficient fair exchange and certified e-mail protocols.

Keywords: Certified e-mail, contract signing, digital signatures, fair exchange, proof of knowledge, public-key cryptography

16 A secure marketplace for mobile Java agents
Kay Neuenhofen, Matthew Thompson
May 1998 **Proceedings of the second international conference on Autonomous agents AGENTS '98**
Publisher: ACM Press
Full text available: pdf(889.69 KB) Additional Information: full citation, references, citings, index terms

Keywords: agent architectures, mobile agents, security

17 Applied cryptography II: Stateful public-key cryptosystems: how to encrypt with one 160-bit exponentiation
Mihir Bellare, Tadayoshi Kohno, Victor Shoup
October 2006 **Proceedings of the 13th ACM conference on Computer and communications security CCS '06**
Publisher: ACM Press
Full text available: pdf(235.26 KB) Additional Information: full citation, abstract, references, index terms

We show how to significantly speed-up the encryption portion of some public-key cryptosystems by the simple expedient of allowing a sender to maintain state that is re-used across different encryptions.In particular we present stateful versions of the DHIES and Kurosawa-Desmedt schemes that each use only 1 exponentiation to encrypt, as opposed to 2 and 3 respectively in the original schemes, yielding the fastest discrete-log based public-key encryption schemes known in the random-oracle and stan ...

Keywords: cryptography, public-key encryption

18 Flash mixing

Markus Jakobsson

May 1999 **Proceedings of the eighteenth annual ACM symposium on Principles of distributed computing PODC '99**

Publisher: ACM Press

Full text available: pdf(962.64 KB) Additional Information: full citation, references, citings, index terms

19 Security and Middleware Services: Efficient and secure keys management for wireless mobile communications

Roberto Di Pietro, Luigi V. Mancini, Sushil Jajodia

October 2002 **Proceedings of the second ACM international workshop on Principles of mobile computing POMC '02**

Publisher: ACM Press

Full text available: pdf(190.14 KB) Additional Information: full citation, abstract, references, index terms

This paper presents an efficient algorithm for the secure group key management of mobile users. The most promising protocols to deal with group key management are those based on logical key hierarchy (LKH). The LKH model reduces to logarithmic size the resources needed: computation time, message exchanged, and memory space. In the framework of the LKH model, we present a new protocol LKH++ that outperforms the other proposed solutions in the literature. Such performance improvements are obtained ...

Keywords: backward secrecy, collusion, cryptography, distributed algorithms, forward secrecy, key distribution, key generation, key management protocol, network dynamics management, secure multicast, wireless communications

20 A key-chain-based keying scheme for many-to-many secure group communication

Dijiang Huang, Deep Medhi

November 2004 **ACM Transactions on Information and System Security (TISSEC)**, Volume 7 Issue 4

Publisher: ACM Press

Full text available: pdf(311.81 KB) Additional Information: full citation, abstract, references, index terms

We propose a novel secure group keying scheme using *hash chain* for *many-to-many* secure group communication. This scheme requires a *key predistribution center* to generate multiple hash chains and allocates exactly one hash value from each chain to a group member. A group member can use its allocated hash values (secrets) to generate group and subgroup keys. Key distribution can be offline or online via the key distribution protocol. Once keys are distributed, this scheme enab ...

Keywords: Hash chain, key chain, many-to-many secure group communication, secure group communication

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next